NIS-2-Umsetzungsgesetz in Kraft

Handlungsempfehlungen für betroffene Unternehmen

9. Dezember 2025

Die Bundesregierung hat am 5. Dezember 2025 ein Gesetz zur Umsetzung der NIS-2-Richtlinie (EU) 2022/2555 verabschiedet. Das Gesetz ist unmittelbar in Kraft getreten und sieht keine Umsetzungsfrist vor. Mit dem „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" setzt die Bundesregierung vorläufig einen Schlussstrich unter einen langwierigen Prozess zur grundlegenden Überarbeitung des deutschen Cybersicherheitsrechts (zu dem holprig verlaufenen Prozess, siehe unsere Briefings vom 7. Februar 2025 und 01. August 2025). Unternehmen, die in bestimmten Sektoren tätig sind und dabei gesetzlich festgelegte Schwellenwerte mit Blick auf Mitarbeiter, Umsatz und Bilanz überschreiten, fallen künftig unter die neuen Kategorien „wichtige Einrichtungen" und „besonders wichtige Einrichtungen". Dazu zählen unter anderem Betreiber kritischer Infrastrukturen, digitale Dienste sowie Hersteller kritischer Produkte. Eine detaillierte Auflistung findet sich in § 28 BSI-Gesetz (*BSIG*).

Nach Schätzungen der Bundesregierung werden zukünftig ungefähr 14.500 Unternehmen von den NIS-2 Anforderungen an Netz und an Netz- und Informationssysteme, erweiterte Meldepflichten und eine höhere Verantwortung der Geschäftsführung betroffen sein. Für eine erste Orientierung, ob ein Unternehmen prinzipiell unter die neuen Regelungen fällt, kann niedrigschwellig und kostenlos ein dafür vom BSI bereitgestelltes Tool für die Betroffenheitsprüfung genutzt werden.

Was kommt jetzt auf die adressierten Unternehmen zu?

Unternehmen, die als wichtige Einrichtungen und besonders wichtige Einrichtungen im Sinne des BSIG einzustufen sind, unterliegen insbesondere den folgenden Verpflichtungen:

- **Registrierungspflicht**: Besonders wichtige Einrichtungen, wichtige Einrichtungen und Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich binnen drei Monaten als NIS-2-Unternehmen zu registrieren (siehe § 33 BSIG). Das BSI empfiehlt betroffenen Unternehmen sich bereits jetzt bei dem neuen bundesweit einheitlichen Unternehmenskonto (Mein Unternehmenskonto, MUK) anzumelden, das auf dem ELSTER-Portal basiert. Mit einem derartigen Unternehmenskonto soll dann eine Registrierung im neuen BSI-Portal möglich sein, das am 6. Januar 2026 freigeschaltet und die zentrale Meldestelle für erhebliche Sicherheitsvorfälle sein wird.

- **Neue Meldepflichten durch dreistufiges Melderegime**: Die betroffenen Unternehmen müssen IT-Sicherheitsvorfälle künftig in drei Stufen melden:
    - unverzügliche Erstmeldung, spätestens binnen 24 Stunden (§ 32 Abs. 1 Nr. 1 BSIG)
    - Zwischenbericht mit Details innerhalb von 72 Stunden (Bestätigung und/oder Aktualisierung des Vorfalls nach (§ 32 Abs. 1 Nr. 2, 3 BSIG) sowie
    - Abschlussbericht spätestens nach einem Monat (§ 32 Abs. 1 Nr. 4 BSIG-E).

  Für Betreiber kritischer Anlagen gelten zudem die zusätzlichen Berichtspflichten des § 32 Abs. 3 BSIG.

- **Implementierung von Risikomanagementmaßnahmen und Dokumentation:** Für betroffene Unternehmen werden zukünftig in § 30 Abs. 2 BSIG eine Reihe von Maßnahmen zum Management von Cybersicherheitsmaßnahmen vorgeschrieben. Dazu zählt etwa die in § 30 Abs. 2 Nr. 10 BSIG vorgesehene Pflicht zur Verwendung von Multi-Faktor-Authentifizierung oder anderer sicherer Kommunikationswege.

Kritische Komponenten als zentrales Streitthema

In den letzten Monaten war insbesondere noch über den Umgang mit **kritischen Komponenten** diskutiert worden, also konkret mit Bauteilen, deren Ausfall oder Manipulation den Betrieb lebenswichtiger Infrastrukturen gefährden könnte. Die nun gefundene Lösung sieht in § 41 BSIG ein **zweistufiges Verfahren** vor:

1. **Liste kritischer Komponenten**: Das Bundesministerium des Inneren (BMI) legt im Einvernehmen mit den zuständigen Ressorts eine Liste solcher Komponenten fest. Bei diesem Vorgang können die Ministerien ihre Interessen einbringen.

2. **Untersagung riskanter Bauteile**: Das BMI kann künftig den Einsatz bestimmter Komponenten eigenständig untersagen und muss dabei andere Ressorts lediglich „ins Benehmen setzen“, also informieren.

Diese Regelung wurde maßgeblich durch Warnungen der Nachrichtendienste vor hybriden Bedrohungen beeinflusst, insbesondere im Zusammenhang mit Bauteilen aus als nicht vertrauenswürdig erachteten Staaten. Betreiber kritischer Anlagen unterliegen nach § 41 Abs. 5 BSIG weitergehenden Mitwirkungspflichten und werden die von ihnen genutzten Komponenten in Zukunft enger mit dem BSI abstimmen müssen.

Ausblick

Die NIS-2 Umsetzung wird bei den betroffenen Unternehmen erst einmal zu höheren Kosten und einem erhöhten Bürokratieaufwand führen. Die Bundesregierung schätzt die zusätzlichen Kosten für die deutsche Wirtschaft auf einmalig 2,2 Milliarden Euro sowie jährlich auf weitere 2,3 Milliarden Euro. Allerdings beträgt das dort durch Cyberangriffe verursachte Gesamtschadensvolumen mehrere hundert Milliarden jährlich. Es bleibt deshalb zu hoffen, dass die bei den betroffenen Unternehmen mit NIS-2 Umsetzung verbundenen Aufwände und Kosten das IT-Sicherheitsniveau so weit erhöhen, dass am Ende auch die deutsche Wirtschaft davon profitiert.

***

BLOMSTEIN wird die weiteren Entwicklungen bei der NIS-2-Umsetzung aufmerksam verfolgen. Wenden Sie sich bei Fragen zum Umgang mit den Entwicklungen im deutschen IT-Sicherheitsrecht jederzeit gerne an Christopher Wolters, Leonard von Rummel und Moritz Schuchert.

BLOMSTEIN | Wir beraten unsere internationalen Mandanten in den Gebieten Kartell-, Vergabe-, Außenwirtschafts- und Beihilferecht sowie ESG in Deutschland, Europa und – über unser globales Netzwerk – weltweit.